

Notice of Allowability	Application No.	Applicant(s)	
	09/838,123	MATCHETT ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment filed on 12/07/2005.
2. ☒ The allowed claim(s) is/are 13-15, 17, 19-29 and 31-32.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input checked="" type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date <u>enclosed</u> |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____ |


KAMBIZ ZAND
PRIMARY EXAMINER

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with **Thomas E. Brown** Reg. No 44,450 on 02/24/2006.

The application has been amended as follows: In the claims

13. (Currently Amended): In a device for performing the Data Encryption Standard (DES) on a block of data bits under control of a DES key and a second cipher key, the in combination with a modified "P" permutation in the "f" function, wherein said modified "P" permutation is selected by a control signal and said control signal utilizes at least some function of a subset of said DES key and said second cipher key.
14. (Currently Amended): The improved device of claim 13, ~~including a~~ wherein said second cipher key to specify specifies said modified "P" permutation.
16. (Canceled)

Art Unit: 2132

17. (Currently Amended): The improved cryptographic device of claim ~~16~~ 13 wherein said control signal can be set so that the improved cryptographic device performs the DES.
18. (Canceled).
19. (Currently Amended) The improved device of claim ~~18~~ 13 wherein said function is time invariant.
20. (Currently Amended) The improved device of claim ~~18~~ 13 wherein said function is time varying.
24. (Currently Amended): The improved cryptographic device of claim 13 including a derivation means to derive said DES key and a said second cipher key from a ~~master~~ third cipher key.
25. (Currently Amended): In a device for performing the "f" function of the Data Encryption Standard (DES), the combination with a modified permutation means to produce a modified permutation replacing the fixed permutation "P" of the DES, said modified permutation means being dependent upon a control means, which utilizes at least some function of a subset of a DES key and a second cipher key.
27. (Currently Amended): A method for performing the Data Encryption Standard (DES) on a block of data bits under control of a DES key and a second cipher key,

Art Unit: 2132

in combination with a modified "P" permutation in the "f" function, comprising the step of:

replacing the "P" permutation in the "f" function by said modified permutation, wherein said modified permutation is at least a function of a subset of said DES key and said second cipher key.

30. (Cancelled).

32. (New): In a device for performing the encrypt process or the decrypt process of the Data Encryption Standard (DES) on a block of data bits under control of a DES key in combination with a modified "P" permutation in the "f" function, wherein said modified "P" permutation is selected by a control signal and said control signal utilizes at least a function of a subset of a DES key and a second cipher key in combination with a non deterministic bit generator so that the said device output is non deterministic.

Allowable Subject Matter

1. **Independent Claims 13, 25 and 27** have been amended. (Examiner Amendment)
2. **New Independent claim 32 has been** added. (Examiner's Amendment)
3. **Claims 16, 18 and 30** have been cancelled. (Examiner's Amendment)
4. Dependent **Claims 14, 17, 19-20 and 24** have been amended. (Examiner's Amendment)
5. **Claims 1-12** have been previously cancelled.
6. **Claims 13-15, 17, 19-29 and 31-32** are allowed.
7. The following is an examiner's statement of reasons for allowance:

Art Unit: 2132

8. With respect to **the independent claims 13, 25 and 27** the art on the record, namely the combination of **Thomas J. Robert and Michael Portz or the combination of Thomas J. Roberts and Michael C. Wood** discloses some of the limitation recited in the independent claims **13, 25 and 27** before the claims were amended.

However independent **claims 13, 25 and 27** are amended by the applicant and limitation from the respective dependent claims has been added and the art on the record does not disclose or suggest this particular added limitation of the respective independent claims **13, 25 and 27** which is recited as follows

“wherein said modified permutation is at least a function of a subset of said DES key and said second cipher key.”

None of the prior art of record taken singularly or in combination teaches or suggests the improved cryptographic device for performing the Data Encryption Standard (DES) with all the limitations recited in respective independent claims in combination with the following functional limitation, wherein said modified permutation is at least a function of a subset of said DES key and said second cipher key

For the reasons provided above, the amended independent claims **13, 25 and 27** are allowed.

9. Referring to **the new independent claims 32, the claim has the similar limitation as that of the independent claims 13, 25 and 27 and is allowed for the same rationale.** Some new features of this particular claims has been checked and no new matter has been introduced. For example feature of this claim limitation such as “non deterministic bit generator so that the said device output is non deterministic” has been checked and support is found at least on page 15 of the original specification.

Art Unit: 2132

10. The dependent claims 14-15, 17, 19-24 which are dependent on the independent claim 13 and the dependent claim 26 which is dependent on the independent claim 25 and finally the dependent claims 28, 29 and 31 which are dependent on independent claim 27 being further limiting to the independent claims, definite and enabled by the specification are also allowed.

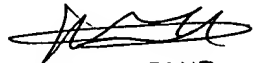
Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am --4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


KAMBIZ ZAND
PRIMARY EXAMINER

Application/Control Number: 09/838,123

Page 7

Art Unit: 2132

A handwritten signature in black ink, appearing to read 'Kambiz Zand', with a horizontal line drawn underneath it.

KAMBIZ ZAND
PRIMARY EXAMINER

SAMSON LEMMA

S.L.

02/28/2006